III. REMARKS

1. Claim 3 is amended to clarify the terminology used in the claim.

2. Claims 3-5 are not anticipated by Chang.

Claim 3 is amended to clarify that the "authentication" data can be exchanged "during a call". Chang fails to disclose or suggest the ability to exchange "authentication" data "during a call". Chang only discloses how to conduct an authentication procedure between mobile terminals. Chang proposes a hybrid end-to-end authentication and key agreement (AKA) protocol, which provides authentication and key exchange between both end entities (abstract), but does not exchange authentication data during a call as claimed by Applicant.

In Chang, in order to eliminate the requirements of a large database to hold all the session keys which are used to establish connections for conventional approaches, and the heavy load contributed by the exponential computations of ID-based authentication protocol, Chang proposes a hybrid protocol and user cache to maintain the session keys set up by the modified ID-based authentication protocol (see e.g. pg. 1252 beginning of section 2).

Applicant's invention aims to improve the authentication procedure in mobile communication networks between two subscribers. According to the invention, the mobile subscriber is authenticated and an encryption key is agreed using user-to-user data exchange. This can be done during a call setup or call. It is important to note that the authentication ends up when it is completed, but it may continue even when the call is

established. In case the authentication procedure continues when the call is established, there could be e.g. a beep signal to indicate that the authentication procedure has been completed and the line is safe now. More specifically, the mobile station B is authenticated by the mobile station A constructing and sending to the mobile station B a message M_1. The mobile station B receives the message M_1, constructs and sends a message M_2 to the mobile station A. The mobile station A receives the message M_2, checks the validity of the information in the message M_2, and if the information is verified valid the mobile station A accepts to share a shared key K with mobile station B. The mobile station A constructs and sends the message M_3 to the mobile station B. The mobile station B receives the message M_3 and verifies the validity of the information, and if the information is valid the mobile station B accepts the sharing of the shared encryption key K with the mobile station A.

However, Chang does not mention that the authentication procedure can be continued when the call has already been established i.e. "during a call" as recited in claim 3. The initial part of the authentication protocol means the procedure in which the portable unit (entity) authenticates with the VSD and sets up a session key. A temporary identity is also assigned to the entity. By basic protocol it is meant the procedure in which an efficient protocol is provoked (p. 1254, first column, last paragraph).

Tables 5 and 6 of Chang merely disclose the challenge and protocol. However, there is nothing in these sections, or any other section of Chang that would suggest that authentication data is exchanged "during a call". Section 2.1 of Chang merely states that the authentication is complete when the called entity verifies and returns its response to the caller. (pg. 1256, lines

1-4). Chang only proposes the use of two protocols, end-to-end authentication and link authentication. (pg. 1256, section 4). However, nowhere does Chang recite, or even teach, that authentication data can be exchanged "during a call", as recited in claim 3. Since this feature is not explicitly recited in Chang, claim 3 cannot be anticipated.

The Examiner states that the Applicant has failed to "explicitly identify specific claim limitations" to define a patentable distinction over Chang. However, claim 3 explicitly recites exchanging authentication data "during a call". This disclosure cannot be found in Chang. Although the Examiner identifies that Chang discloses end-to-end authentication, the Examiner has not identified any portion of Chang that teaches exchanging "authentication" data "during a call". For example, on page 1254, second column, Chang states that whenever "a call is made after an entity roams into a VSD, an authentication process is initiated". Chang only states here that after successful authentication, "VSD forwards the challenge of caller to called entity if both entities do not have a shared key". In the reference to FIG. 5, Chang states on page 1256, first column, that given that there is already a session key shared by the portable unit and VSD, VSD first identifies the portable unit before allowing it to access the mobile network. Table 6 shows how the VSD identifies the caller entity. However, nothing here discloses or suggests that "authentication" data is exchanged "during a call".

Thus, since Chang does not disclose or suggest the exchange of "authentication" data "during a call", claim 3 should be allowable. Claims 4 and 5 should be allowable at least by reason of their respective dependencies.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Geza C. Ziegler, Jr.
Reg. No. 44,004

11 May 2005
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted by facsimile to (703) 872-9306 the date indicated below, addressed to the Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Date: 11 May 2005

Signature: M. Baye

Name: Meaghan Baye